Complete Cyber

ROLLING STOCK - CYBERSECURITY

Cyber Onions

Company Overview

“We excel in transforming the cybersecurity landscape for businesses. Our expertise lies in addressing the most complex cybersecurity challenges that organisations face in today's rapidly evolving digital world”

- Security Architecture Services
- Security Testing (Vulnerability & Penetration Testing)
- Audit & Risk Assessments (Cybersecurity assurance)
- Security Monitoring
- Asset Monitoring & Management

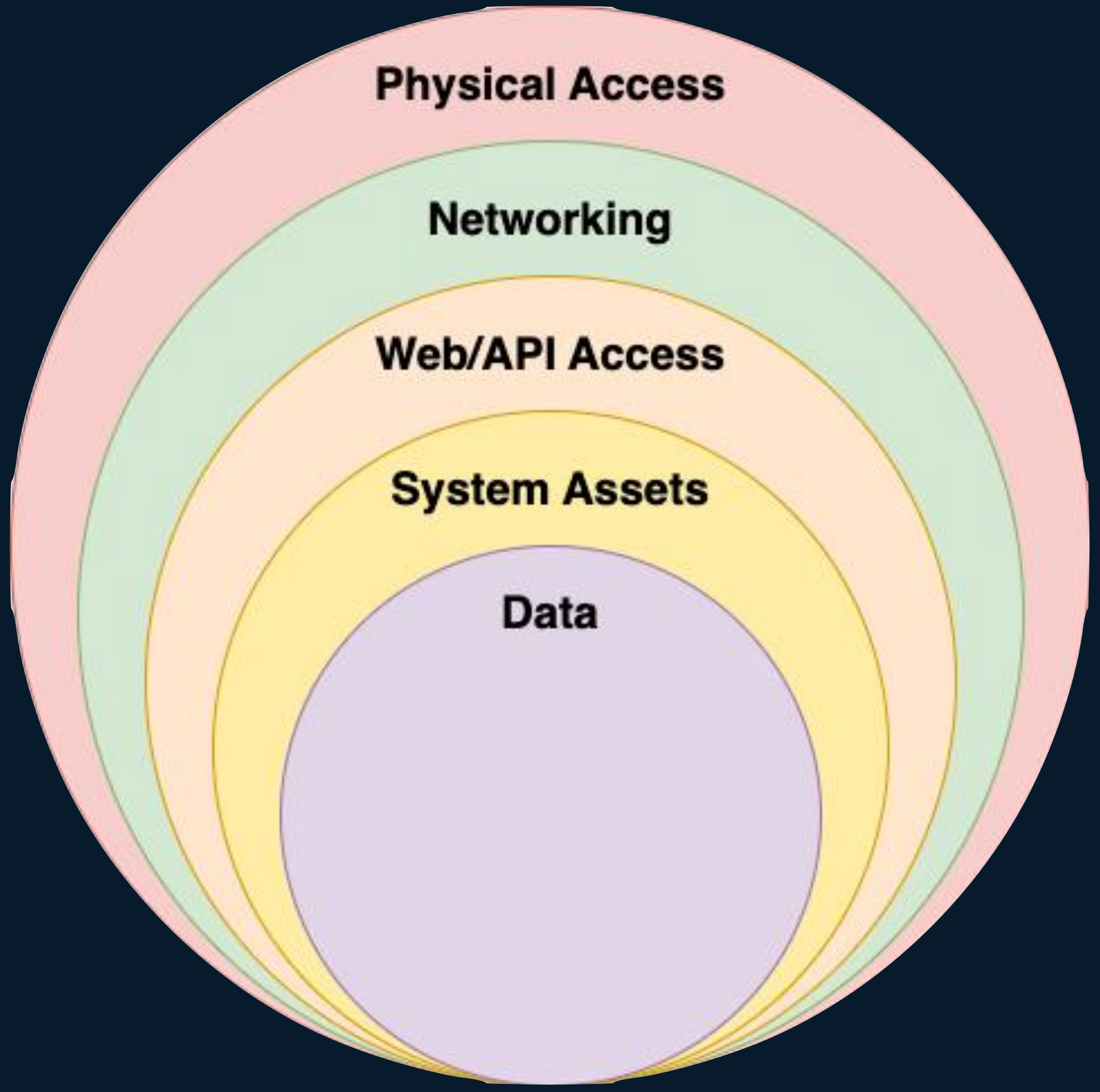
~/Users/evanjones: whoami

- Security Lead Architect / Business Developer
- Started as a Graduate in Transport for London - London Underground Ltd (LUL)
- Systems Engineer with Software/Electronic/Integration Experience
- Progressed into Cybersecurity during LUL
- Setup and manages Complete Cyber +10 Years

Rolling Stock Overview & Onions

Complete Cyber

- Modern Rolling Stock is generally built with fault-tolerant ethernet networks (Ring)
- Supported by Serial Communications (RS422/485, CAN Bus, MVP etc.) for Safety Critical Systems
- Wireless Communication Methods (Passenger/Staff WiFi & 4/5G Remote Connectivity)



- Most Digital Systems (IT, IOT & OT) can be contextualised into an Onion
- A review into this approach to understand the breakdown of forms of security threats and risks for Rolling Stock systems
- MITRE ATT&CK CNI Matrix used for contextual threat-to-risk analysis

Physical Security

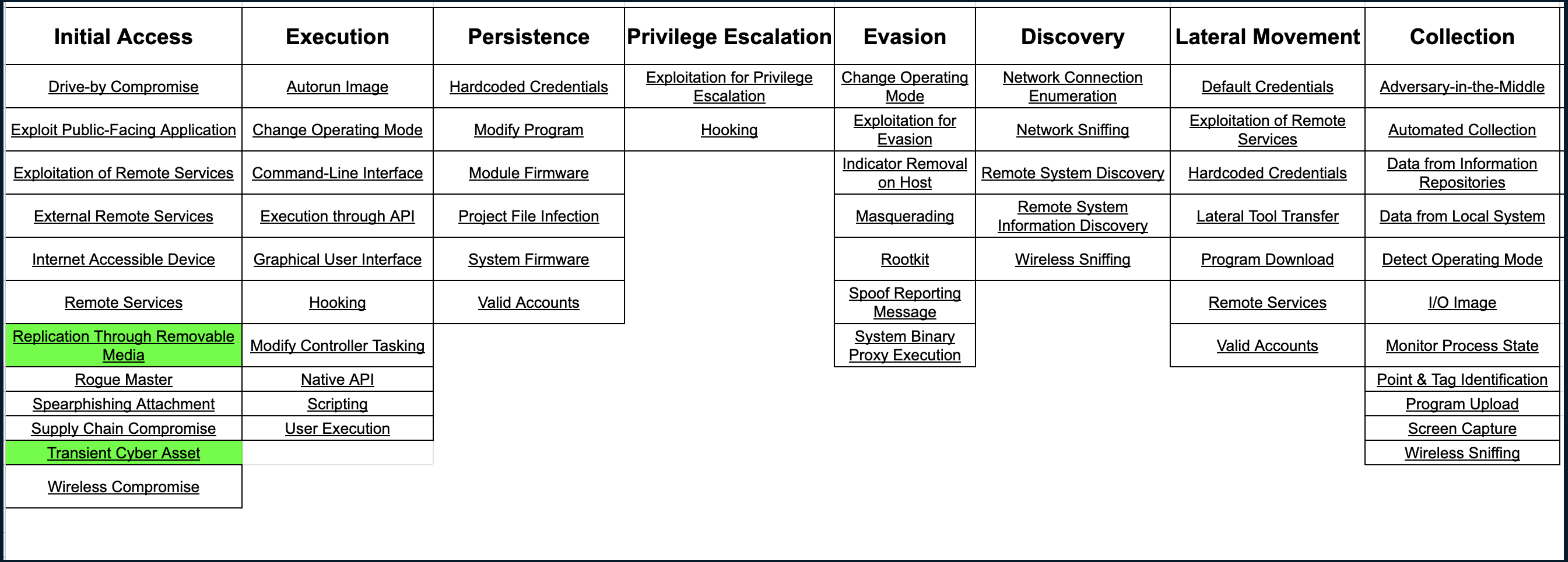
Threats

- Public User uses generic key-shape for panel access and removes cable
- Public or informed User accesses panel removal in discretion (Toilet example)
- Lack of physical inspection methods (Manual & Automated)

Physical Security Cont.

Risks

- Detriment Network performance (Availability) and Functional Performance
- Force Emergency Breaks On (when travelling at speeds of excess 125 kph)
- Obtain initial persistence for reconnaissance

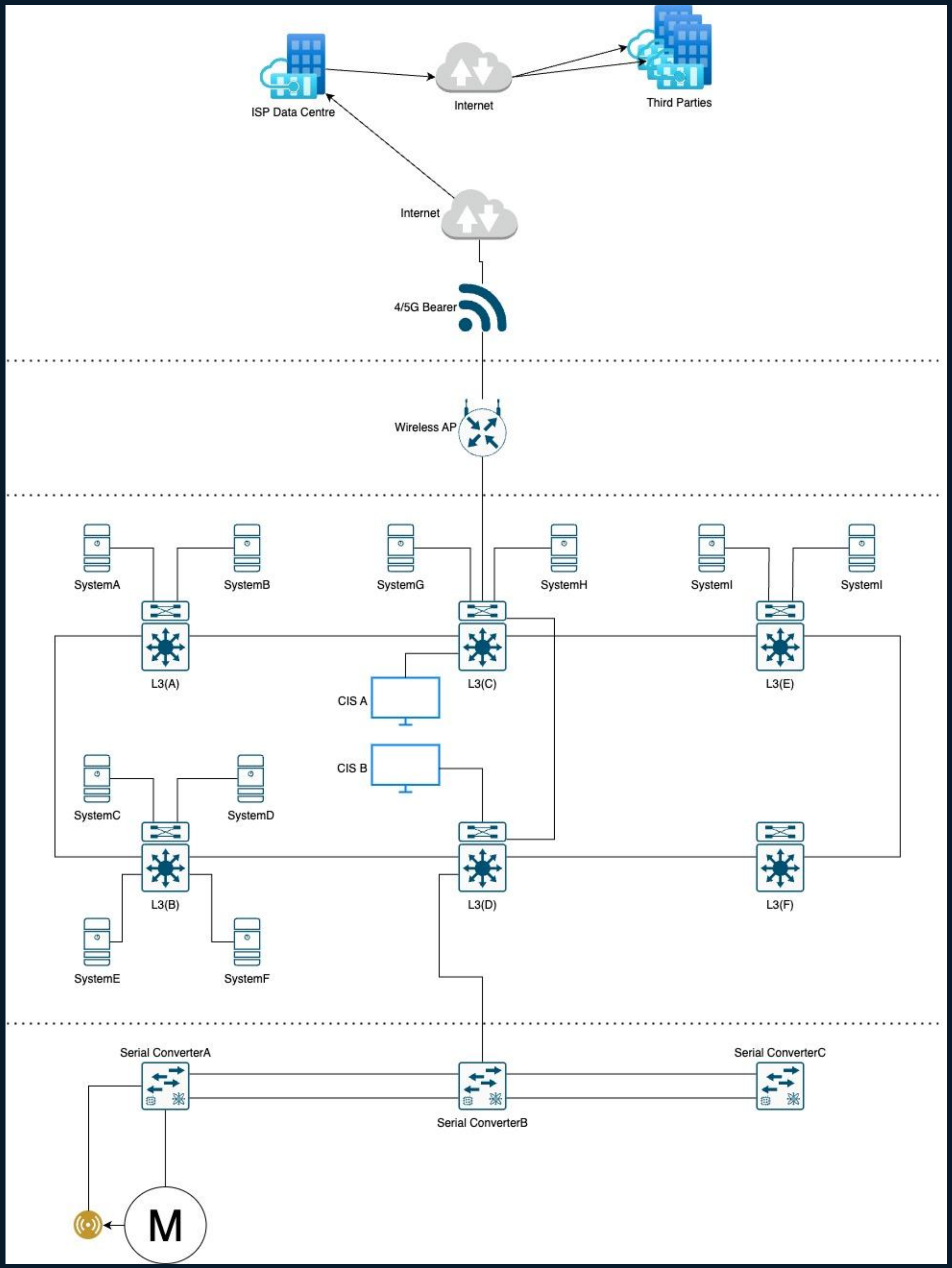


Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State
Rogue Master	Native API						Point & Tag Identification
Spearphishing Attachment	Scripting						Program Upload
Supply Chain Compromise	User Execution						Screen Capture
Transient Cyber Asset							Wireless Sniffing
Wireless Compromise							

Network Systems

Threats

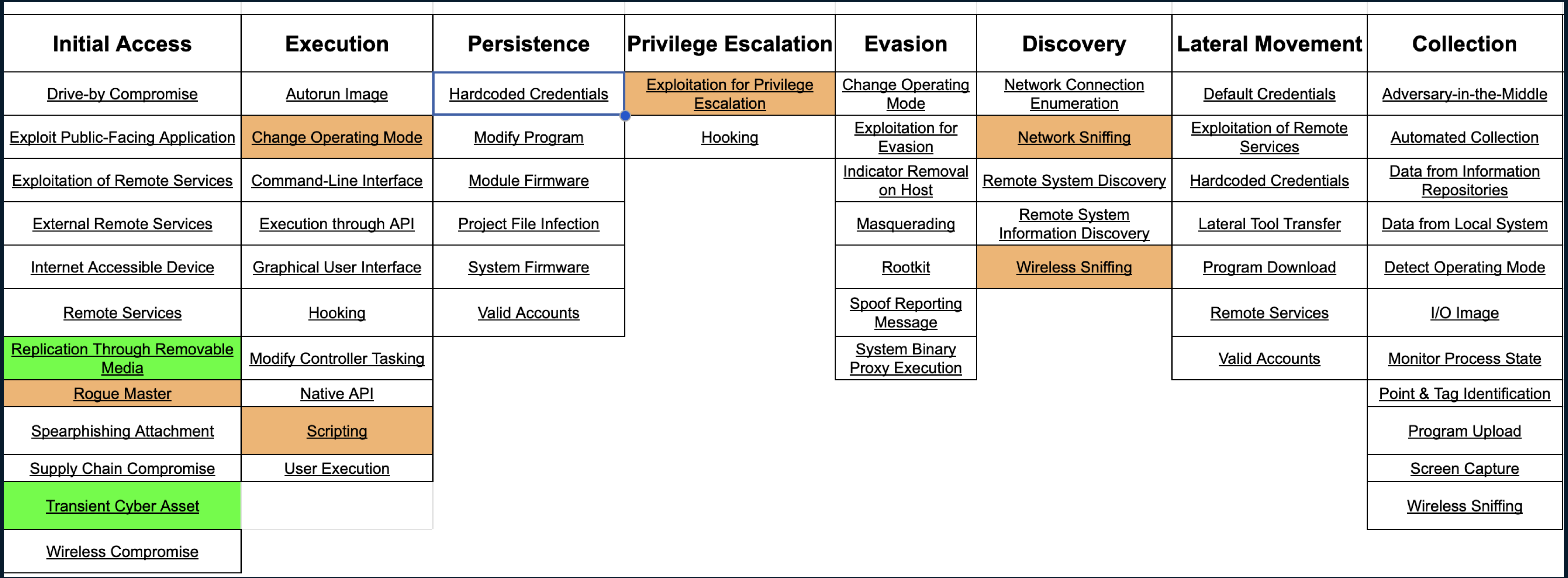
- Flat network for lateral access movements
- Default or weak credentials on network devices (switches)
- Lack of network ACLs for support in segregation
- Poor network management



Network Systems Cont.

Risks

- Lateral movement within network with no-detection in place
- Network system compromised due to weak or limited authentication methods
- Change in network control routing attacks



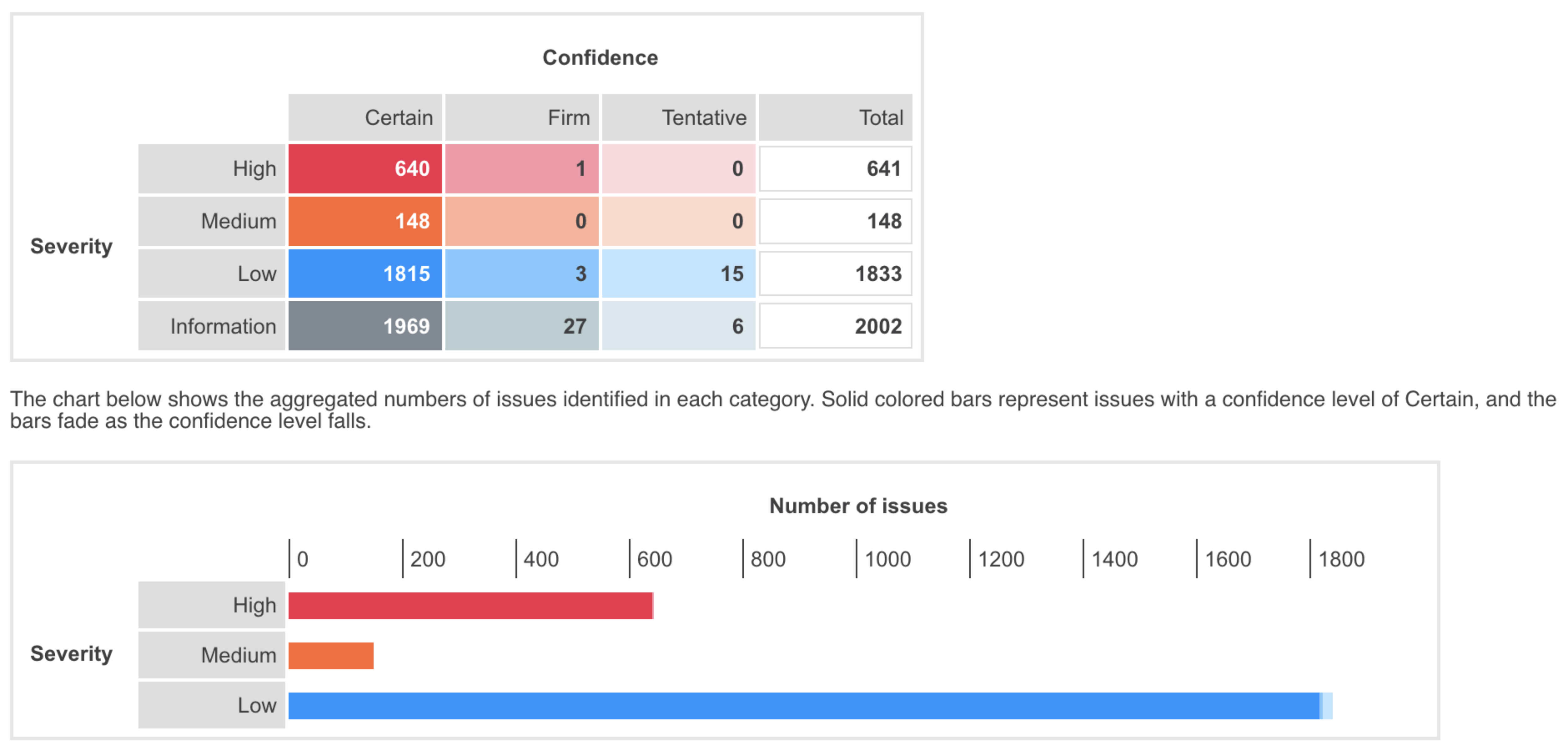
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State
Rogue Master	Native API						Point & Tag Identification
Spearphishing Attachment	Scripting						Program Upload
Supply Chain Compromise	User Execution						Screen Capture
Transient Cyber Asset							Wireless Sniffing
Wireless Compromise							

Web & API Access

Complete Cyber

Threats

- Exposed Services with lack of Authentication and Authorisation in place
- Enumeration of Services
- Lack of Integrity and Confidentiality in Software Development for Web & API systems



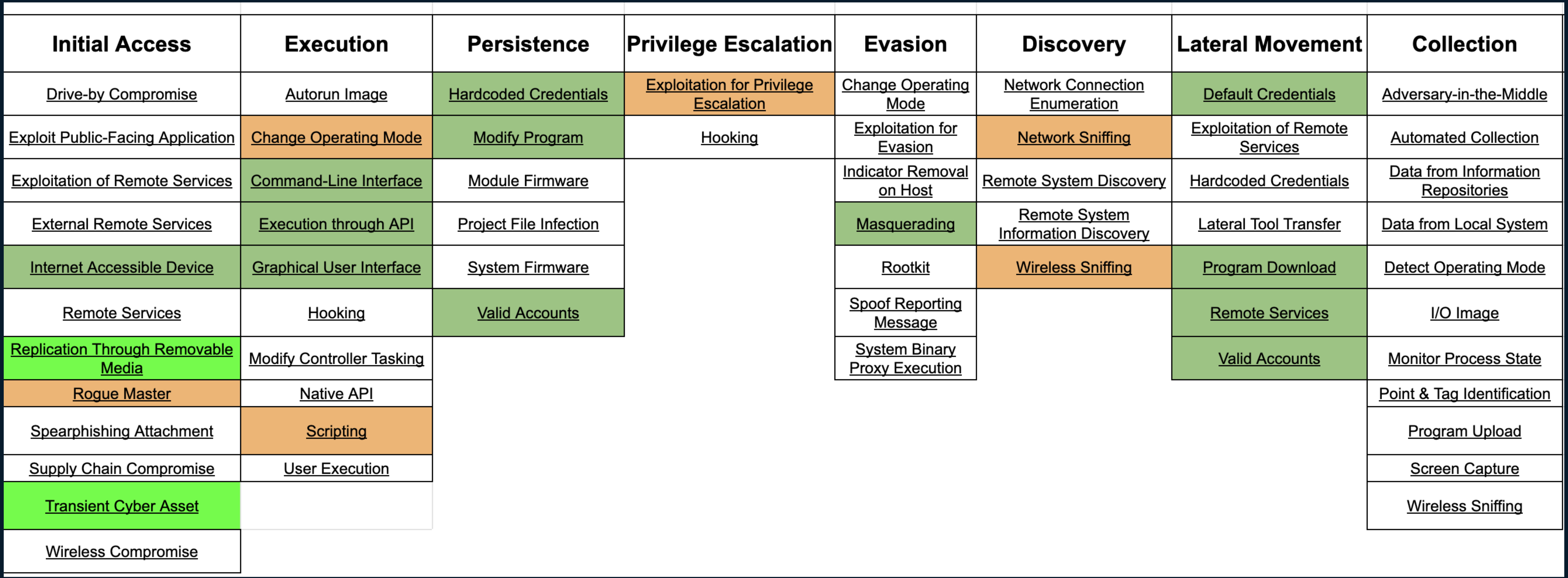
		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	640	1	0	641
	Medium	148	0	0	148
	Low	1815	3	15	1833
	Information	1969	27	6	2002

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.

Web & API Access

Risks

- Easy Authentication and enumeration of Web services and API
- Privilege abuse through weak authentication and authorisation methods
- Web shell (server-side) execution attacks for downloading or establishing backdoors

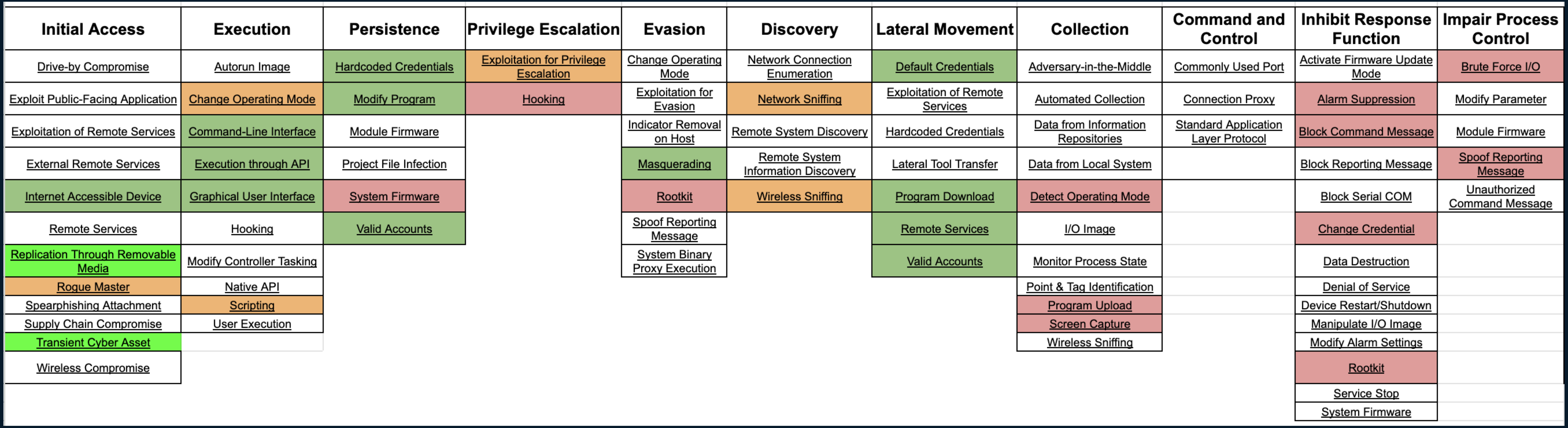


Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State
Rogue Master	Native API						Point & Tag Identification
Spearphishing Attachment	Scripting						Program Upload
Supply Chain Compromise	User Execution						Screen Capture
Transient Cyber Asset							Wireless Sniffing
Wireless Compromise							

System Asset Compromise

Threats

- Limited system hardening in place making initial attack and escalation easy
- Lack of system monitoring and detection makes System modifications possible
- Interception of Services and Data become accessible

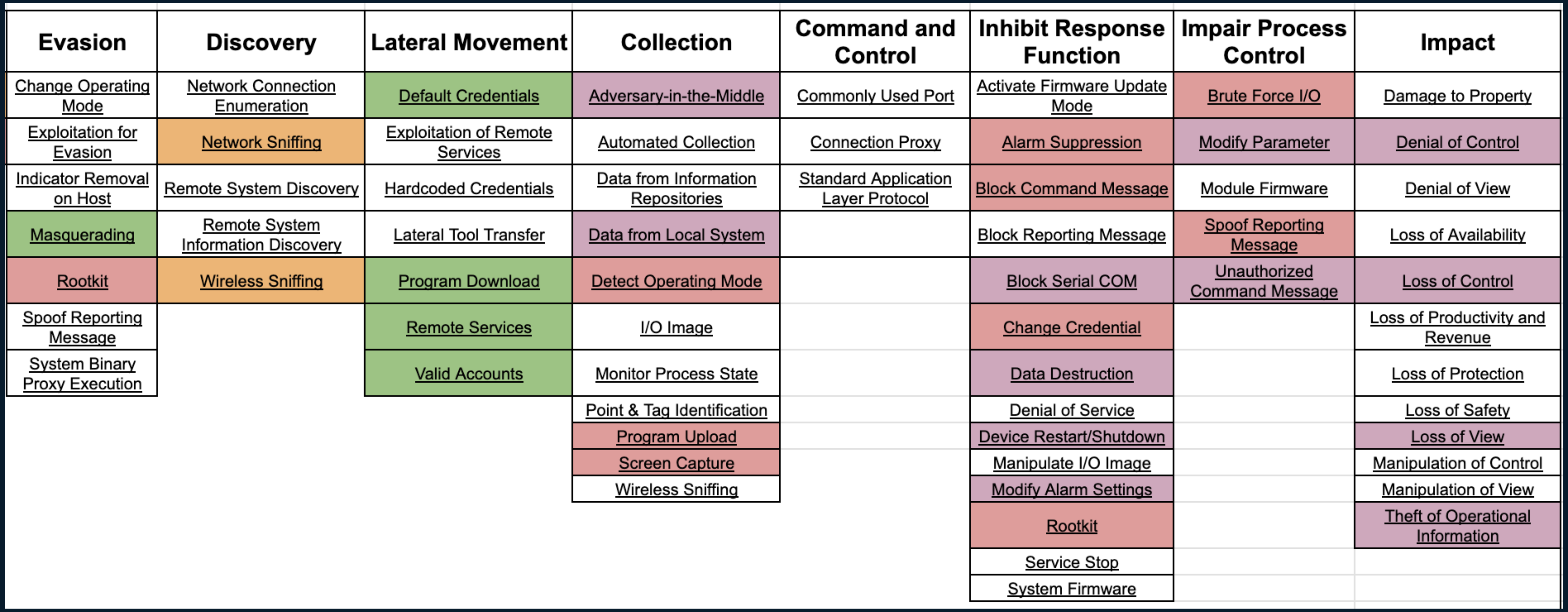


Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential	
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction	
Rogue Master	Native API						Point & Tag Identification		Denial of Service	
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown	
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image	
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings	
Wireless Compromise									Rootkit	
									Service Stop	
									System Firmware	

Data Access & Manipulation

Threats

- Core data integrity and confidentiality is accessible and unprotected
- Implementation of a ‘Trust-All’ approach can allow for sniffing and data extraction
- Data parameter modification and manipulation



Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
			Point & Tag Identification		Denial of Service		Loss of Safety
			Program Upload		Device Restart/Shutdown		Loss of View
			Screen Capture		Manipulate I/O Image		Manipulation of Control
			Wireless Sniffing		Modify Alarm Settings		Manipulation of View
					Rootkit		Theft of Operational Information
					Service Stop		
					System Firmware		

Key Take Aways

Complete Cyber

1. Implement Security Architecture for ‘Secure-by-Design’ through OEMs (EU Cyber Requirement)
   I. Assign Product/Project Manager with Cybersecurity responsibilities
   II. Adopt 62243-3-3 for System and 62443-4-1/2 for Product Security (Supply-Chain)

2. Ensure continuous testing during the Design & Build of Rolling Stock (EU Cyber Requirement)
   I. Consider better or improved security within the Software Development Process
   II. Enforce ad-hoc testing during the design process (Digital Twin testing)

3. Ensure relevant controls (Technology, Process & People) are built into the programme of a new Design & Build (NISD/2 Requirement & EU Cybersecurity Act)
   I. Factor budgets for security tooling and documentation processes for people including training
   II. Speak with the Cybersecurity OT Supply-Chain on support for addressing controls

4. Undertake continuous testing and monitoring of your Rolling Stock (NISD/2 Requirement)
   I. Ensure services offering monitoring and response are added into bids and offered to Clients
   II. Tooling to undertake continuous monitoring and discovery
   III. Assignment of external party for continuous testing & internal

Complete Cyber

Thank You
Contact Us For Support

Complete Cyber LinkedIn Page

completecyber.co.uk

contactus@completecyber.co.uk

Very Light Rail, National Innovation Centre,
Zoological Dr, Dudley DY1 4AW, First Floor